BY KEVIN M. SAVETZ

Web Cookies

Harmless Convenience, Or Insidious Invasions Of Privacy?

Your Web browser is keeping notes about you. Don't fret, it's not as bad as it sounds. After all, how can something with an innocuous name like "cookies" be bad?

A cookie is simply a note to itself that a Web site leaves on your computer's hard drive. You know how your applications—Microsoft Word, Netscape, and other programs that you use—create preferences files? Cookies are preferences files for Web sites.

Any information that you give to a site can be stored in a cookie, so that next time you visit that site (later that day or even months in the future) the site can read its cookie and remember your preferences. For instance, if you tell the site that you prefer to see the "frames" version of Web pages and that you use Windows NT, the site can stash that data in a cookie. The next time around, it will use frames and tell you about new Windows NT software.

Or you might click your way to the classical area of an online music store using cookies; the store duly notes your penchant for Pachelbel, and on your next visit the site highlights classical releases. Unless you have set your browser to warn you when cookies are added, you probably won't even realize the process has occurred.

Cookies can only store information that you give to the Web site. This includes the basics like what parts of the site you visit. But a site can't get your email address, for example, unless you give it to them.

So, many experts view cookies as mostly harmless. But some folks don't like them—they see cookies as a potential invasion of privacy. Give your credit card number to a Web site, and there's no reason the site can't keep your card info in a cookie to speed your next order.

Privacy advocates wonder if Web sites can snoop on cookies left by other sites. (After all, you don't want *www.shyster.com* to steal credit card info that was stored by another Web site.) With up-to-date Web browsers, this isn't possible.

But cookies work on the Web site's terms, not yours. The site decides what information to jot in a cookie and how to use it. Some users just don't want sites tracking them. Me, I don't mind it much. The sites don't know who I am, nor do they have my email address. I'm just a nameless, faceless Web surfer.

Cookie Central *(http://www.cookiecentral.com)*, a great site devoted to the use and abuse of cookies, has this to say about privacy: "Some people do not like a file that may contain a cookie with information about where they have been, and what they do, if they can stop it. This type of information that is invaluable to some companies.... Cookies can be used to track you on the Net, what sites you go to, what you like, and so on." Indeed, at least one company uses cookies to track the sites that you visit, then deliver targeted advertising banners.

Cookie Control

For privacy advocates and the paranoid, a cottage industry of cookie-crunching software has cropped up. Utilities with names like Crumbler and CookieCrusher will give you better control of your browser's use of cookies, or just erase all the cookies stored on your computer. (By the way, even without your intervention, cookies don't stay around, clogging your hard drive forever. They can be set by a Web site to expire after a certain date.)

Password-protected sites can use cookies to store your username and password necessary for logging in—so deleting your cookies can make it a little more difficult to log in to those sites.

Will you suffer dire consequences by deleting cookies or shutting them off altogether? Some sites will forget what ads you've looked at (big deal) and others will forget your preferences. Password-protected sites can use cookies to store your username and password necessary for logging in—so deleting your cookies can make it a little more difficult to log in to those sites.

In Netscape Navigator and Communicator 4.0, you can control how the browser handles cookies. Pick Preferences from the Edit menu, then click on Advanced. You can accept all cookies (the default), accept only cookies that get sent back to the site you're visiting (a more secure alternative if you're worried about advertisers tracking you,) or don't accept cookies at all (the choice of militant anti-cookie surfers).

You can also tell the browser to warn you every time a site places a cookie on your computer. I find this rather tedious—when the cookie warning dialog box pops up, it interrupts the flow of using the Web.

Microsoft Internet Explorer 4 does not include the option to disable cookies entirely, but there is the option to warn you before a cookie is set. You can activate this by choosing Options from the View menu, choosing Advanced and unchecking the "don't warn before accepting cookies" box.

More information is available at Andy's Cookie Notes *(http://www.illuminatus.com/cookie.fcgi)*. There you'll find links, a very good description of how cookies work, and info on using cookies on your own Web site if you are so inclined. ■

Copyright © 1998 by Kevin M. Savetz. All rights reserved.